REMARKS

Claims 1-46 are pending in the present application. Claims 1, 7, 8, 11, 16-20, 25, 26, 32, 33, 36 and 41-46 have been amended herewith. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

Applicants also would like to acknowledge and thank the Examiner for the telephonic interview on September 21, 2004. While no agreement was reached, the technical merits of the present invention were discussed.

I. Specification

The Examiner notes the use of Java on page 8 of the application, and states it should be capitalized wherever it appears and be accompanied by the generic terminology. Applicants have reviewed the use of Java on page 8 is it appears to comply with the Examiner's requirements. If this objection is maintained, further clarification is requested as to what is required by Applicants in this regard.

The Examiner states the proprietary nature of trademarks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks. Applicants respond by showing that the proprietary nature of the Java trademark is expressly acknowledged in the application at page 8, lines 12-13.

Finally, the Examiner requests Applicants' cooperation in correcting any specification errors which Applicants may become aware of, and Applicants have amended such Specification herewith.

II. Claim Objection

A. The Examiner objected to Claims 1, 20, 26 and 45, stating the phrase "a available resources" needs to be corrected. Applicants have amended such claims accordingly to eliminate this phraseology.

PAGE 16/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

B. The Examiner objected to Claims 19 and 44, stating that "identified" lacks proper antecedent basis. Applicants have amended such claims accordingly to eliminate this word.

Therefore, the objection to the claims has been overcome.

III. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-2, 4-9, 11-27, 29-34 and 36-46 under 35 U.S.C. § 102 as being anticipated by US Patent 5,612,682 to DeLuca et al. This rejection is respectfully traversed.

With respect to Claim 1, Applicants urge that the cited reference does not teach the claimed steps of (i) responsive to a request to perform a cryptographic operation, dynamically selecting one of a software process and a hardware process within the data processing system for performing the cryptographic operation based on a policy, or (ii) performing the cryptographic operation using the selected process. As can be seen, a selection is made between a software and hardware process for performing a cryptographic operation in response to a request to perform such cryptographic operation. In contrast, the cited reference does not teach selection between two types of cryptographic processes responsive to a request to perform a cryptographic operation. Rather, the cited reference uses a fixed cryptographic process - there is no selection between two different types (software and hardware) of cryptographic processes. While the reference alludes to software applications and hardware modules which can be authorized for end-user usage, these software applications and hardware modules do not perform any type of cryptographic operation, but instead perform such things as electronic mail services, spread sheet applications and investment finance services (DeLuca Col. 1, lines 18-29). The cited reference also teaches an authorization technique for authorizing these (non-cryptographic) software applications and hardware modules, but this authorization does not entail selecting between a software process and hardware process to be used as a part of the authorization. Rather, a search is made of internal authorization records of processes which have been authorized for use (Col. 7, line 39 – Col. 8, line 39). There is no selection between multiple differing types of cryptographic

PAGE 17/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

processes as a part of this authorization. The cited reference also teaches encryption being used for data transmission (Col. 5, lines 6-65), but again this is a fixed scheme and there is no teaching of a selection between multiple differing types of cryptographic processes as a part of this encryption/decryption technique.

Thus, it has been shown that Claim 1 is not anticipated by the cited reference, as every element of the claimed invention is not identically shown in a single reference.

Applicants initially traverse the rejection of Claims 2 and 4-9 for reasons given above with respect to Claim 1 (of which Claims 2 and 4-9 depend upon).

Further with respect to Claim 2, Applicants show that the cited reference does not teach the claimed feature of "wherein the policy includes selecting the one based on available resources to perform the cryptographic operation". As can be seen, Claim 2 details specifics of the policy that is used to select between cryptographic processes. In rejecting Claim 2, the Examiner cites DeLuca Col. 9, line 38 – Col. 10, line 15 and Col. 6, lines 19-25 as teaching this claimed feature. Applicants urge that the passage cited beginning at DeLuca Col. 9 describes details of a security element 315 that is used for processing authorization of software and hardware modules. This passage describes whether or not to authorize access to a software or hardware module, but does not teach selecting *between* a software and hardware process that is actually used to perform a cryptographic operation, and thus does not teach that such (missing) selection is based on a policy that selects the one based on available resources to perform the cryptographic operation, as claimed. Thus, Claim 2 is further shown to not be anticipated by the cited reference.

Further with respect to Claim 6 (and dependent Claims 7 and 8), Applicants urge that the cited reference does not teach the claimed feature of "wherein the cryptographic operation is an encryption of data using a key". In rejecting Claim 6, the Examiner cited DeLuca Col. 9, line 38 – Col. 10, line 15. Applicants show that this passage describes details of a security element for processing *authorization* of software and hardware modules. In contrast, Claim 6 is directed to *encryption*. Authorization and encryption are not equivalent functions. According to The American Heritage® Dictionary of the English Language, Fourth Edition published by Houghton Mifflin Company:

PAGE 18/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

au·thor·i·za·tion *n.*

1. The act of authorizing. See synonyms at permission.
2. Something that authorizes; a sanction

en·crypt *tr.v.* en·crypt·ed, en·crypt·ing, en·crypts

1. To put into code or cipher.
2. *Computer Science.* To alter (a file, for example) using a secret code so as to be unintelligible to unauthorized parties

Since authorization and encryption mean very different things, a teaching of process authorization, as taught by the passage cited by the Examiner in rejecting Claim 6, does not teach the claimed encryption of data. Thus, Claim 6 (and dependent Claims 7 and 8) is further shown to not be anticipated by the cited reference.

Still further with respect to Claim 7, Applicants urge that the cited reference does not teach the claimed feature of "wherein the step of performing the cryptographic operation includes converting the key to a form useable by the selected process". In rejecting Claim 7, the Examiner states that this claimed feature is taught by DeLuca at Col. 10, lines 1-15 and lines 55-67. Applicants show error in such assertion, as the passage cited at DeLuca Col. 10, lines 1-15 teaches calculation of a random CRC using a process size. A process size is not an encryption key, and thus the teaching of calculating a random CRC using a process size does not teach *converting a key* to a usable form. Nor does the passage cited at Col. 10, lines 55-67 overcome such deficiency. This passage merely states that the hardware or software process is allowed to be performed upon receipt of an authorization message. There is no teaching of any type of conversion of a key that is used to encrypt data, as claimed. Thus, Claim 7 is further shown to not be anticipated by the cited reference.

Still further with respect to Claim 8, Applicants urge that the cited reference does not teach the claimed feature of "wherein the key is a hardware key and the selected process is the software process and further comprising converting the hardware key into a software form useable by the software process for performing the cryptographic operation". In rejecting Claim 8, the Examiner states that this feature is taught by DeLuca at Col. 10, lines 1-15 and lines 55-67. Applicants show error in such assertion,

PAGE 19/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

as the passage cited at DeLuca Col. 10, lines 1-15 teaches calculation of a random CRC using a process size. A process size is not an encryption key, and thus the teaching of calculating a random CRC using a process size does not teach *converting a key* (used to *encrypt* data) to a usable form. Nor does the passage cited at Col. 10, lines 55-67 overcome such deficiency. This passage merely states that the hardware or software process is allowed to be performed upon receipt of an authorization message. There is no teaching of converting a hardware key (used to *encrypt* data) into a software form useable by a software process for performing a cryptographic operation. Thus, Claim 8 is further shown to not be anticipated by the cited reference.

Further with respect to Claim 9, Applicants urge that the cited reference does not teach the claimed feature of "wherein the policy comprises a set of rules used to minimize available resources consumed in performing the cryptographic operation". In rejecting Claim 9, the Examiner cites DeLuca Col. 14, lines 1-25 and Col. 15, lines 55-65. As to the DeLuca passage cited at Col. 14, Applicants show that this passage describes installation of a hardware and software module in a portable communication device. The passage goes on to describe that the hardware/software module can be registered by sending an authorization form and proof of purchase receipt. Once added to the portable communication device, the user may request execution of the process, or alternatively the processor of the communication device checks for the presence of an authorization record. There is no teaching of any set of rules which are used to minimize available resources consumed *in performing the cryptographic operation*. To the extent the Examiner is equating process authorization to be the same as the claimed cryptographic operation, this authorization process does not use a set of rules that are used to minimize available resources consumed during such authorization process. Similarly, skipping authorization altogether, as per step 610, does not teach use of a set of rules used to minimize available resources consumed *in performing a cryptographic operation*, as no authorization operation is performed at all – i.e. it is skipped altogether. Thus, there is no teaching of a set of rules used to minimize available resources consumed in performing the cryptographic operation, as claimed. Thus, Claim 9 is further shown to not be anticipated by the cited reference.

PAGE 20/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

With respect to Claim 11, Applicants urge that the cited reference does not teach the claimed steps of (i) responsive to a request to perform a cryptographic operation, dynamically selecting from one of a software process and a hardware process within the data processing system for performing the cryptographic operation based on available resources to perform the cryptographic operation, or (ii) performing the cryptographic operation using the selected process. As can be seen, the selection between the software and hardware process for performing the cryptographic operation is based on available resources to perform the cryptographic operation. In rejecting Claim 11, the Examiner merely asserts that DeLuca teaches selecting one of a software and hardware process based *on a policy,* which policy results in available resources. Claim 11 is not merely directed to a policy which *results in* available resources (a reactive consequence), but rather the actual selection of the policy is based upon available resources to perform the cryptographic operation (an active a priori state of the available resources). The cited reference does not teach selection between a hardware and software cryptographic process based on such available resources, and thus Claim 11 is shown to not be anticipated by the cited reference.

Applicants initially traverse the rejection of Claims 12-19 for reasons given above with respect to Claim 11 (of which Claims 12-19 depend upon).

Further with respect to Claim 12, Applicants urge that the cited reference does not teach the claimed feature of "wherein the cryptographic operation is one of a message digest and a public-private key encryption". In rejecting Claim 12, the Examiner cited DeLuca Col. 5, lines 5-45 as teaching this claimed feature. Applicants show that there, DeLuca discusses a single type of encryption process, and thus this passage does not teach selecting between a software process and a hardware process within the data processing system for performing the cryptographic operation, where the cryptographic operation is one of a message digest and a public-private key encryption. In addition, there is no teaching of either (i) a message digest being the cryptographic operation, or (ii) a public-private key encryption being the cryptographic operation. At best, the cited passage merely teaches use of a secure encryption key. In contrast, Claim 12 explicitly recites a public-private key encryption. Thus, Claim 12 is further shown to not be anticipated by the cited reference.

PAGE 21/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

Further with respect to Claim 15, Applicants traverse for similar reasons to those further reasons given above regarding Claim 6.

Further with respect to Claim 16, Applicants traverse for similar reasons to those further reasons given above regarding Claim 7.

Further with respect to Claim 17, Applicants traverse for similar reasons to those further reasons given above regarding Claim 8.

Further with respect to Claim 18, Applicants urge that the cited reference does not teach the claimed feature of "wherein the key is a software key and the selected process is the hardware process and further comprising converting the software key into a hardware form". In rejecting Claim 18, the Examiner cites DeLuca Col. 10, lines 1-15 and lines 55-67. Incredibly, this is the identical passage cited by the Examiner as teaching wherein the key is a *hardware* key and the selected process is the *software* process and further comprising converting the hardware key into a software form useable by the software process for performing the cryptographic operation (as recited in Claim 8). Claim 18 states that the key is a *software key* and the selected process is a *hardware process*. It is logically inconsistent for the Examiner to cite the same passage as teaching that the key used to encrypt data is both a hardware key as well as a software key, and that the selected process is both a software process and a hardware process.

In addition to this logical inconsistency, Applicants also show that these cited passages merely teach calculation of a random CRC using a process size. A process size is not a key, and thus the teaching of calculating a random CRC using a process size does not teach *converting a key* used to encrypt data to a usable form. Nor does the passage cited at Col. 10, lines 55-67 overcome such deficiency. This passage merely states that the hardware or software process is allowed to be performed upon receipt of an authorization message. There is no teaching of converting a software key (used to *encrypt* data) into a hardware form useable by a hardware process for performing a cryptographic operation. Thus, Claim 18 is further shown to not be anticipated by the cited reference.

Applicants traverse the rejection of Claim 20 (and dependent Claims 21-24) for similar reasons to those given above with respect to Claim 1.

PAGE 22/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

Applicants traverse the rejection of Claim 25 for similar reasons to those given above regarding Claim 11.

Applicants traverse the rejection of Claim 26 (and dependent Claims 27 and 29-34) for similar reasons to those given above with respect to Claim 1.

Applicants further traverse the rejection of Claim 27 for similar reasons to those further reasons given above with respect to Claim 2.

Applicants further traverse the rejection of Claim 31 for similar reasons to those further reasons given above with respect to Claim 6.

Applicants further traverse the rejection of Claim 32 for similar reasons to those further reasons given above with respect to Claim 7.

Applicants further traverse the rejection of Claim 33 for similar reasons to those further reasons given above with respect to Claim 8.

Applicants further traverse the rejection of Claim 34 for similar reasons to those further reasons given above with respect to Claim 9.

Applicants traverse the rejection of Claim 36 (and dependent Claims 37-44) for similar reasons to those given above regarding Claim 11

Applicants further traverse the rejection of Claim 37 for similar reasons to those further reasons given above with respect to Claim 12.

Applicants further traverse the rejection of Claim 40 for similar reasons to those further reasons given above with respect to Claim 6 and 15.

Applicants further traverse the rejection of Claim 41 for similar reasons to those further reasons given above with respect to Claim 7 and 16.

Applicants further traverse the rejection of Claim 42 for similar reasons to those further reasons given above with respect to Claim 8 and 17.

Applicants further traverse the rejection of Claim 43 for similar reasons to those further reasons given above with respect to Claim 18.

Applicants traverse the rejection of Claim 45 for similar reasons to those given above with respect to Claim 1.

Applicants traverse the rejection of Claim 46 for similar reasons to those given above with respect to Claim 11.

PAGE 23/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50

Therefore, the rejection of Claims 1-2, 4-9, 11-27, 29-34 and 36-46 under 35 U.S.C. § 102 has been overcome.

IV. 35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 3, 10, 28 and 35 under 35 U.S.C. § 103 as being unpatentable over US Patent 5,612,682 to DeLuca et al. in view of US Patent 5,835,600 to Rivest. This rejection is respectfully traversed for reasons given above with respect to Claim 1.

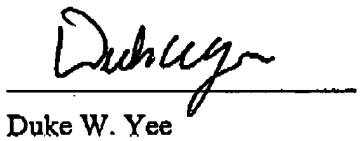
Therefore, the rejection of Claims 3, 10, 28 and 35 under 35 U.S.C. § 103 has been overcome.

V. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 9/23/04

Respectfully submitted,



Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 367-2001
Attorneys for Applicants

PAGE 24/24 * RCVD AT 9/23/2004 3:55:28 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/8 * DNIS:8729306 * CSID:9723672008 * DURATION (mm-ss):06-50